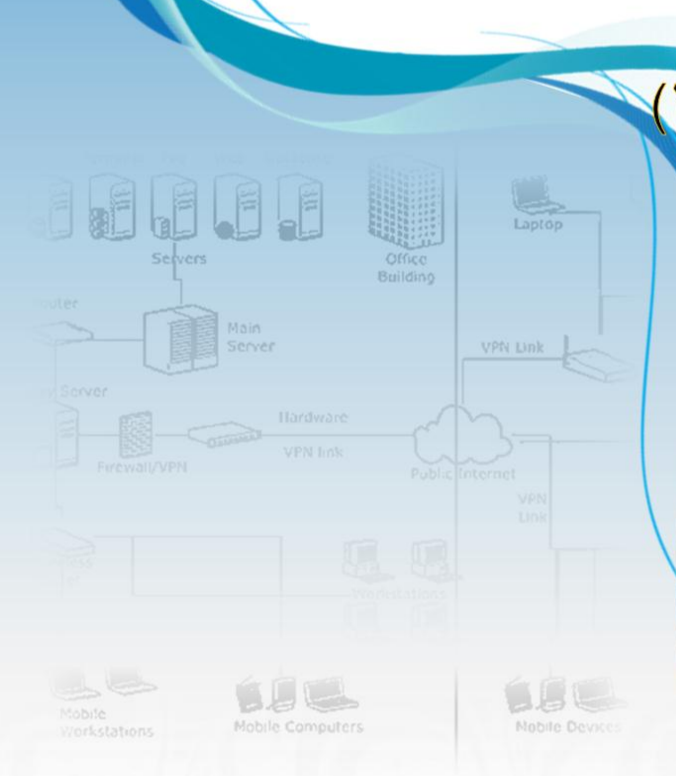


جامعة أم درمان الإسلامية
كلية الهندسة
قسم الهندسة الكهربية و الإلكترونية

أمن الشبكات السلكية

WIRED NETWORKS SECURITY

إعداد :
الوسيلة إبراهيم موسى (٢٩)
بشار بشير على عثمان(٣٠)
بشرى رحمه إمام (٣١)





بسم الله الرحمن الرحيم



✦ تعريف الشبكات الحاسوب :

شبكة اتصالات الحاسب هي مجموعة من الحواسب المرتبطة مع بعضها بطريقة ربط معينة عبر وسائط تتبع في ذلك لمعايير مختلفة ، في أبسط أشكالها تتكون شبكة الحاسب من جهازين متصلين ببعضهما بواسطة سلك ، و يقومان بتبادل البيانات.

✦ أمن الشبكات :

تتلخص أهداف خدمات تأمين الشبكات فيما يلي:

١ - **الخصوصية أو السرية Privacy or Confidentiality** :

٢ - **المصداقية Authentication**

٣ - **تكامل البيانات Data Integrity**

٤ - **الإتاحية Availability**

قد يترتب على توفير الخدمات السابقة ان يجد المستخدمون القانونيون للشبكة صعوبة في الوصول الى المصادر التي يحق لهم التمتع بها كنتيجة للقيود التي تفرضها الاساليب المستخدمة. لذا يجب ان يراعى في تصميم تلك السبل الا تحول دون اتاحة المصادر لمستخدميها القانونيين.

✦ ملخص البحث :

سنتناول في هذا البحث بإذن الله عن أمن الشبكات السلكية في طبقة التطبيقات و برتكولاتها **SSL** و **TLS** و **SMB** و كذلك تقنية **HASH** .

كذلك سوف نتحدث عن أمن طبقة الشبكة و النظام العملاق **IPSce** و برتوكولاته و الطرق التي يستخدمها في الشبكة . ثم نتحدث عن الجدار الناري لعنصر مهم للحماية في الشبكات السلكية و كذلك **DMZ** لتوفير حماية للشبكة السلكية عند توصيلها مع الشبكة العالمية **(INTERNET)** .



ثم ندلف إلي نظام كشف التسلل **IDS** و تقنياته و الطرق المستخدمة لكشف التسلل

و في ذيل البحث تناولنا طرق الحماية في المكونات المادية للشبكات السلكية متمثلة في فلترة كرت الشبكة و حماية الأسلاك – الكوابل– التي تعتبر الوسيط الناقل في عملية الإتصال داخل الشبكة السلكية

✦ أمن الشبكات السلكية **Wired Networks Security** :

الأمن في طبقة التطبيقات و طبقة العرض:

بعد التقدم والتطور الذي حصل في عالم الحماية ، وبعد تطور أساليب المخترقين في عملياتهم وتنوعها كـــــMan-IN-THe-Midle و الـــSniffing والـــــRelaying والكثير غيرها .

الهجمات على طبقة التطبيقات Application Layer Attacks

حيث تعمل هذه الهجمات على التاثير على النظام المستخدم في أجهزة الشبكة وأيضا تعمل على التأثير على البرامج المستخدمة في الشبكة، ومن الأمثلة عليها الفيروسات والديدان التي تنتشر بفعل ثغرات في الأنظمة أو البرامج أو حتى أخطاء المستخدمين في الشبكة السلكية. يعمل الIPSec –سيتم تناوله لاحقا بشيء من التفصيل– على الحماية من ذلك بكونه يعمل على طبقة IP Layer فيعمل على إسقاط أي حزمة بيانات لا تتطابق والشروط الموضوعة لذلك ، لذا فتعمل الفلاتر على إسقاطها وعدم إيصالها للأنظمة أو البرامج في الشبكة.

لذلك كان لا بد من إيجاد طريقة امنه لتخطي هذه الأمور وخصوصا في الأمور الحساسة كالتجارة الإلكترونية وعمليات كشف الحسابات وغيرها ، فكان لابد من طريقه لتامين ذلك ، فتم تطوير تقنيه SSL : **S**ecure **S**ocket **L**ayer

أمِّنت هذه الطريقة قيام اتصال امن مشفر Encrypted بين أجهزة الشبكة المحلية (السلكية) ، ضمن تعقيدات متفاوته فمنها الBit٤٠ ومنها bit١٢٨ ،، فتم استخدام الـــSSL لتشفير وحماية قنوات الاتصال التي تنتقل عبرها البيانات مثل SMTP أو الـــDatabase communications .

ثم ظهرت تقنيه مشابه له و هي الTLS : Transport Layer Security وهي تقنيه محسنه من الSSL ولكنهما يختلفان في طريقة اداء العمليه ،، والطريقتان تحتاجان للشهادات الالكترونيه Certificates او بالاحرى Web-based Certificates .



وظهرت تقنيه اخرى داخل الشبكه المحلية السلكية ، وهي SMB Signing .

: SMB : **S**erver **M**essage **B**lock

هي الـــــ packets التي يتم إرسالها بين السيرفر والأجهزة – المرتبطة بالشبكة– في عملية المشاركة في الملفات وغيره Sharing ،، وللحماية من طريقة سرقة المعلومات اثناء مرورها في الأسلاك Man In The Middle MITM وهذه الطريقة تدعى SMB Signing ،، يتم بواسطتها إضافة الHash .

The Hash : عباره عن مجموعة ارقام واحرف عشوائيه يتم توليدها بطرق حسابيه معقده جدا من نص عندك (ممكن رساله) او من حزمة بيانات ، او حتى من بيانات حجمها ١٠٠٠ ميجا، الهاش طوله وشكله ثابت لا يتغير ، هو لا يشفر ، وانما هو للحفاظ على مصداقية البيانات.

بمعنى انه إن أراد احد إرسال رسالة، فانه يخرج الهاش الخاص بها و يرسله مع الرسالة، و الشخص الذي يستقبل الرسالة يقارن الهاش الذي استلمه بالهاش الخاص بالرسالة، فان تم تعديل الرسالة و لو بإضافة مسافة ، فان الهاش سيختلف.

باختصار طريقة الهاش يتم من خلالها استخلاص رمز معين حسب حسابات رياضيه من الرسالة ، ومن الأمثلة عليه MD4 , MD5 , SHA-1 ويتم تشفير هذا الHash وأضافته للرسالة وبذلك نحافظ على صحة الرسالة Message or Packet Integrity .

- و المشكلة الكبرى تكمن في أن جميع هذه الوسائل تعمل على الApplication Layer في الــــــOSI Model أي أن وظائفها محدده جدا ، لا تستطيع تشفير إلا ما بنيت لأجله ، لذلك كان لا بد من ابتكار طريقة تمكننا من تشفير كل Packet تصدر من أي جهاز داخل الشبكة السلكية .

الأمن في طبقة الشبكة و النقل:

- ✓ تم ابتكار تقنيه الــ**IP Security** وهي تقنيه تعمل على الـــــIP Layer في الــ DOD Model أو الــNetwork Layer في الــــــOSI Model .

بمعنى انه يقوم بتشفير كل شيء يصدر عن الجهاز ويرسله على الشبكة Network بما أن الـــــNetwork Layer هي الجهة التي من خلالها يمرر كل شيء للشبكة .فالـــــIPSec تقنيه توفر الموثوقيه والصحة والتشفير لكل شيء يمر من خلالها على مستوى الـــــIP Packet .

IPSec Protocols

الـــIPsec هو طريقه وليس بروتوكول كما يخطأ البعض ، لكن للـــIPSec بروتكولات رئيسيان هي :

أولا: AH : Authentication Header

يستخدم الAH في توقيع الرسائل والبيانات Sign ولا يعمل على تشفيرها Encryption ، حيث يحافظ فقط على ما يلي للمستخدم :

١. **موثوقية البيانات Data authenticity** :

أي أن البيانات المرسلة من هذا المستخدم هي منه وليست مزوره أو مدسوسة على الشبكة .

٢. **صحة البيانات Data Integrity** : أي أن البيانات المرسلة لم يتم تعديلها على الطريق (أثناء مرورها على الأسلاك) .

٣. **عدم إعادة الإرسال Anti-Replay** :

وهذه الطريقة التي ستخدمها المخترقون حيث يقومون بسرقة كلمة السر وهي مشفره ويقومون بإعادة إرسالها في وقت آخر للسيرفر وهي مشفره وطبعا يفك السيرفر التشفير ويدخل المستخدم على أساس انه شخص آخر،، فالIPSec يقدم حلولا لمنع هذه العملية من الحدوث.

٤. **حمايه ضد الخداع Anti-Spoofing protection** :

ويوفر ايضا الIPSec حماية ضد الخداع من قبل المستخدمين ، مثلا يمكن ان يحدد مدير الشبكه السلكية انه لا يسمح لغير المستخدمين على الsubnet 192.168.0.X بينما يسمح لحاملي الهويه ١٩٢.١٦٨.١.x من دخول السيرفر ، فيمكن للمستخدم ان يغير الIP Address خاص به ، لكن الIPSec يمنع ذلك .(وايضا يمكنك القياس على ذلك من خارج الشبكه الى داخلها) يكون لكل الحزمه Packet موقعه Digitally signed.

هذا هو الشكل العام لحزمة البيانات Pack et التي تمر في بروتوكول AH



ثانياً: ESP : Encapsulating Security Payload

يوفر هذا البروتوكول التشفير والتوقيع للبيانات معا Encryption and Signing ، ومن البديهي اذا ان يستخدم هذا البروتوكول في كون المعلومات سريه Confidential او Secret ، او عند ارسال المعلومات عن طريق Public Network . في الشبكة السلكية .

يوفر الESP المزايا التاليه:

١. **Source authentication** :

وهي مصداقية المرسل ، حيث كما وضحنا في مثال الSpoofing انه لا يمكن لاي شخص يستخدم الIPSec تزوير هويته ،(هوية المرسل).

٢. **التشفير للبيانات Data Encryption** :

حيث يوفر التشفير للبيانات لحمايتها من التعديل أو التغيير أو القراءة .

٣. **Anti-Replay** : موضحه في الAH .

٤. **Anti-Spoofing Protection** : موضحه في ال AH.

ثالثاً: IKE : Internet Key Exchange

الوظيفة الاساسيه لهذا البروتوكول هي ضمان الكيفيه وعملية توزيع ومشاركة المفاتيح Keys بين مستخدمي الIPSec ، فهو بروتوكول الــnegotiation اي النقاش في نظام الIPSec كما انه يعمل على تاكيد طريقة الموثوقيه Authentication والمفاتيح الواجب استخدامها ونوعها (حيث ان الIPSec يستخدم التشفير DES٣ وهو عباره عن زوج من المفاتيح ذاتها يتولد عشوائيا بطرق حسابيه معقده ويتم اعطاءه فقط للجهة الثانيه ويمنع توزيعه وهو من نوع Symmetric Encryption اي التشفير المتوازي ويستخدم تقنية الPrivate Key .

IPSec modes : أي طرق أو أنواع الـــــIPSec التي يستخدمها في الشبكة . ينقسم الIPSec الى نظامين او نوعين وهما :

١. نظام النقل Transport Mode
٢. نظام النفق Tunnel Mode .

أ. نظام النقل Transport Mode

يستخدم هذا النظام في الشبكه المحليه LAN : Local Area Network حيث يقدم خدمات التشفير للبيانات التي تتطابق والسياسه المتبعه في الـــIPSec بين أي جهازين في الشبكة ، أي يوفر Endpoint-to-Endpoint Encryption فمثلا اذا قمت بضبط سياسة الـــIPSec على تشفير جميع الحركة التي تتم على المنفذ ٢٣ وهو منفذ الـــTelnet – حيث أن الTelnet ترسل كل شيء مثلما هو دون تشفير Plain Text – فاذا تمت محادثه بين السيرفر أو مستخدم ومستخدم آخر على هذا المنفذ فان الـــIPSec يقوم بتشفير كل البيانات المرسلة من لحظت خروجها من جهاز المستخدم إلى لحظه وصولها إلى السيرفر.

يتم تطبيق هذا النظام Transport Mode في الحالات التالية :

أولا : المحادثة التي تتم بين الأجهزة في نفس الشبكة الداخلية الخاصة Private LAN .

ثانيا: المحادثة التي تتم بين جهازين ولا يقطع بينهما Firewall – سيتم أخذ نبذة عنه لأهميته في الأمن – حائط ناري يعمل عمل الـــNAT .

NAT : **N**etwork **A**ddress **T**ranslation

نظام يمّكن الـــFirewall من استبدال جميع عناوين الIPs في الشبكة الداخلية عن حزمة البيانات Packet واستبدالها في عنوان Public IP آخر ، ونستفيد من ذلك هو أننا لن نحتاج سوى إلى عنوان IP واحد ، وأيضا انه يقوم بإخفاء عناوين الأجهزة عن شبكة الإنترنت للحماية من الاختراق الخارجي .

❀ الجدار ناري firewall :

ظهرت تقنية الجدار الناري في أواخر الثمانينات عندما كانت الإنترنت تقنية جديدة نوعاً ما من حيث الاستخدام العالمي.

تعريف الجدار الناري:

هو عبارة عن جهاز (Hardware) أو نظام (Software) يقوم بالتحكم في مسيرة و مرور البيانات (Packets) في الشبكة أو بين الشبكات و التحكم يكون إما بالمنع أو بالسماح ، وقد تم تطوير الـــ**firewall** إلى:



➢ الجيل الأول: مفلترات العبوة (Packet Filters)

قام مهندسون من (DEC) بتطوير نظام فلترة عرف باسم جدار النار بنظام فلترة العبوة

تعمل فلترة العبوات بالتحقق من "العبوات"(packets) التي تمثل الوحدة الأساسية المخصصة لنقل البيانات بين الحواسيب ، لأن (TCP) و (UDP) في العادة تستخدم مرافئ معروفة إلى أنواع معينة من قنوات المرور، فإن فلتر عبوة "عديم الحالة" يمكن أن تميز و تتحكم بهذه الأنواع من القنوات (مثل تصفح المواقع، الطباعة البعيدة المدى، إرسال البريد الإلكتروني، إرسال الملفات)، إلا إذا كانت الأجهزة على جانبي فلتر العبوة يستخدمان نفس المرافئ الغير اعتيادية.

➢ الجيل الثاني: فلتر محدد الحالة (Stateful Filters)

➢ الجيل الثالث: طبقات التطبيقات (Application Layer Firewall)

عرف باسم "الجدار الناري لطبقات التطبيقات و عرف أيضا بالجدار الناري المعتمد على الخادم النيابي (Proxy server).

ماذا يستطيع أن يفعل الجدار الناري ؟

١- إن الجدار الناري يعتبر النقطة الفاصلة التي تبقي الغير مصرح لهم بدخول الشبكة من الدخول لها و التعامل معها بشكل مباشر و التي تقلل من استغلال ثغرات هذه الشبكة و خدماتها كـ IP spoofing , ARP spoofing , Routing attacks , DNS attacks

٢- يحدد الجدار الناري اتجاه البيانات الصادرة والواردة من و إلى الشبكة.

٣- يحدد الجدار الناري الأنظمة الموثوقة أو (Trusted Systems) و هو الجهاز أو الشبكة أو النظام الموثوق بهم و التي يُسمح لها بالتعامل مع الشبكة .

٤- يقوم الجدار الناري بمراقبة البيانات العابرة من و إلى الشبكة و أيضا تسجيل و تتبع الأحداث و التنبيه عن أي أخطار أو أحداث غريبة تحصل .

✗ ما الذي لا يستطيع أن يفعله الجدار الناري ؟

١- لا يستطيع الجدار الناري الحماية ضد الهجمات التي تعبره ، و التي تعتمد على ثغرات في بروتوكولات لا تستطيع الشبكة الاستغناء عنها .



٢- لا يستطيع الحماية من المخاطر التي داخل الشبكة السلكية نفسها أي من الأفراد الذين هم بطبيعة الحال داخل الشبكة السلكية و قد حصلوا على تلك الثقة التي جعلتهم في داخل الشبكة.

٣- لا يستطيع الجدار الناري الحماية من الفيروسات و الديدان و الاتصال العكسي في الشبكة و التي تنتشر بسرعة و تسبب خطورة على كامل الشبكة السلكية الداخلة حيث تنتقل عبر الرسائل و مشاركة الملفات الخبيثة.

❀ المنطقة المحايدة DMZ

الهدف الأساسي من ابتكار المنطقة المحايدة – و بتعبير آخر المنطقة منزوعة السلاح- هو حماية الشبكة السلكية سواء أكانت محلية أو واسعة أو غيرهما من الهجمات التي تتعرض لها من المخترقين من شبكة الإنترنت و ذلك في حالة توصيل الشبكة مع الشبكة العالمية.

كما نرى في الشكل المجازر أن بإمكان مستخدمي الشبكة العالمية من الاتصال بالمنطقة المحايدة من شبكة المنظمة لكن ليس بإمكانهم الدخول إلى شبكة المنظمة الخاصة.

و في الشكل أيضا نرى جداريين ناريين، الهدف من الجدار الناري الأول بين الشبكة العالمية والمنطقة المحايدة من شبكة المنظمة هو حماية الخوادم الموجودة في المنطقة المحايدة – والتي بطبيعتها لابد أن تكون مرئية للعالم – من الهجمات عن طريق الشبكة العالمية، وهذه الحماية بناءاً على الفلترة كالسماح لبروتوكولات معينة بالمرور مثل (HTTP, HTTPS) ومنع البرتوكولات الأخرى مثل (FTP, Telnet)

و قد ظهرت تقنية أوعية العسل (Honeypots) التي تستخدم في المناطق المحايدة لإبعاد الاختراقات المحتملة على شبكة المنظمة، و هي عبارة عن خوادم مزودة ببرامج و بيانات تظهر و كأنها موثوقة و صحيحة لتوجيه أنظار المخترقين إليها و صرفهم عن الخوادم الحقيقية.

٢. نظام النفق Tunnel Mode .

يتم استخدام هذا النظام لتطبيق الـــIPSec بين نقطتين تكون بالعادة بين راوترين ٢ Routers . اذا يتم استخدام هذا النظام بين نقطتين بعيدتين جغرافيا أي سيتم قطع الإنترنت في طريقها الى الطرف الثاني ، مثل الاتصالات التي تحدث بين الشبكات المتباعدة جغرافيا WAN : Wide Area Network ، يستخدم هذا النظام فقط عند الحاجه لتأمين البيانات فقط أثناء مرورها من مناطق غير امنه كالانترنت ، فمثلا اذا أراد فرعين لشركه ان يقوم بتشفير جميع البيانات التي يتم ارسالها فيما بينهم على بروتوكول FTP : File Transfere Protocol فيتم إعداد الIPSec على أساس ال Tunneling Mode .

❁ بعض المميزات الرئيسية في الـــIPSec والتي جعلته متفوقا على غيره :

فوائده IPSec Benefits

بالإضافة إلي الفائدة التي ذكرناها بأنه يقوم بتشفير كل شيء يصدر عن الجهاز ويرسله على الشبكة Network .

فلقد ظهر ضعف كبير في عملية الEncryption العادية التي تتم بين الأجهزة في الشبكات ، وهذا الضعف تمثل في صعوبة تطبيق هذا الموضوع ، وأيضا استهلاكه للوقت ، أي بطئه الشديد في القيام بعملية التشفير وفكه Encryption and decryption .

فالفائدة الكبرى التي ظهرت في الIPSec هي انه يوفر حماية كامله وواضحة لجميع البروتوكولات التي تعمل على الطبقة الثالث Layer 3 of the OSI Model وما بعد هذه الطبقة ، مثل طبقة التطبيقات Application Layer وغيرها .

يقوم في العادة مدير الشبكة بوضع السياسات التي يريد أن يطبق الـــIPSec عليها بعد دراسة جميع النتائج لهذا التطبيق ، فمثلا يقوم بعمل قائمه للبروتوكولات الواجب تشفيرها كـــ, HTTP , FTP SMTP ويقوم بجمعها معا في ما يسمى سياسه الـــــIPSec أو IPSec Policy . تحتوي هذه السياسة على الفلاتر المتعددة التي يستخدمها الـــIPSec لتحديد أي البروتوكولات يحتاج إلى التشفير Encryption (أي باستخدام ESP) وأيها بحاجه إلى توقيع الكرتوني Digital Signing (أي باستخدام

AH) أو الاثنين معا . فتبعا لذلك كما ذكرنا ، فان أي حزمه من البيانات تمر من خلال هذه المنافذ وتستخدم البروتوكولات المحددة فانه يتم تشفيرها أو توقيعها كما هو محدد . والأفضل في هذه العملية ، أن المستخدم لا يشعر بشيء وغير مطلوب منه عمل شيء ،، وإنما مدير الشبكة يقوم بتطبيق سياسة الIPSec على الDomain أو على أي OU : Organaizational Unit فيتم بشكل تلقائي التشفير وفكه عند ارساله من جهاز وعند وصوله للجهاز الآخر .

- من مميزات الIPSec أيضا هو انه موجود أصلا Built-in في داخل حزمة الIP Packet ، فلذلك هو لا يحتاج لأي إعدادت لانتقاله عبر الشبكة ولا يحتاج لأي أجهزه إضافية لذلك .

✓ كيف يحمي IPSec من الهجمات على الشبكات؟

كما نعرف انه بلا اخذ الأمن بعين الاعتبار ، فان الشبكة السلكية والبيانات التي تمر فيها يمكن أن تتعرض للعديد من أنواع الهجمات المختلفة ، بعض الهجمات تكون غير فعاله Passive مثل مراقبة الشبكة Network Monitering ، ومنها ما هو الفعال Active مما يعني أنها يمكن أن تتغير البيانات أو تسرق في طريقها عبر كوابل الشبكة السلكية. وفي هذا الدرس سوف نستعرض بعض أنواع الهجمات على الشبكات، وكيفية منع IPSec حدوثها أو كيفية الوقاية منها عن طريق الــIPSec .

أولا: التقاط حزم البيانات Eavesdropping, sniffing or snooping

حيث يتم بذلك مراقبة حزم البيانات التي تمر على الشبكة بنصها الواضح دون تشفير Plain text والتقاط ما نريد منها ، ويعالجها الــIPSec عن طريق تشفير حزمة البيانات، عندها حتى لو التقطت الحزمة فانه الفاعل لن يستطيع قراءتها أو العبث بها، لان الطرف الوحيد الذي يملك مفتاح فك التشفير هو الطرف المستقبل(بالإضافة إلى الطرف المرسل) .

ثانيا: تعديل البيانات Data modification

حيث يتم بذلك سرقة حزم البيانات عن الشبكة ثم تعديلها وإعادة إرسالها إلى المستقبل، ويقوم الIPSec بمنع ذلك عن طريق استخدام الهاش Hash ووضعه مع البيانات ثم تشفيرها معا ، وعندما تصل الحزمة إلى الطرف المستقبل فان الجهاز يفحص Checksum التابع للحزمة اذا تمت مطابقته أم

لا، فاذا تمت المطابقة مع الهاش الأصلي المشفر تبين أن الحزمة لم تعدل، لكن اذا تغير الهاش نعرف عندها أن حزمة البيانات قد تم تغييرها.

ثالثا: انتحال الشخصية Identity spoofing

بحيث يتم استخدام حزم البيانات على الشبكة السلكية والتقاطها وتعديلها لتبين هويه المزوره للمرسل، أي خداع المستقبل بهوية المرسل، ويمنع ذلك عن طريق الطرق الثلاثة التي ذكرناها سابقاً والتي يستخدمها الـــIPSec وهي:

- بروتوكول الكيربرس Kerberos Protocol
- الشهادات الإلكترونية Digital Certificates
- مشاركة مفتاح معين Preshared key

حيث لا تتم عملية بدء المحادثة وإرسال البيانات قبل التأكد من صحة الطرف الثاني عن طريق احدى الطرق المذكورة سابقا.

رابعا: DoS -Denial of Service رفض الخدمة أو حجبها

حيث تعمل هذه الهجمة على تعطيل خدمه من خدمات الشبكة للمستخدمين والمستفيدين منها ، مثلا كإشغال السيرفر في الشبكة السلكية بعمل فلود Flood عليه مما يشغله بالرد على هذه الأمور وعدم الاستجابة للمستخدمين في الشبكة. ويعمل الIPSec على منع ذلك عن طريق إمكانيه غلق أو وضع قواعد للمنافذ المفتوحة Ports .

خامسا: MITM -Man In The Middle

من اشهر الهجمات في الشبكات السلكية، وهي أن يكون هنالك طرف ثالث يعمل على سرقة البيانات المرسلة من طرف لآخر وإمكانية العمل على تعديلها أو العمل على عدم إيصالها للجانب الآخر، ويعمل الـــــIPSec على المنع عن طريق طرق التحقق من الموثوقيه والتي ذكرناها سابقا Authentication methods

سادسا: سرقة مفتاح التشفير Key interception

❀ بشكل عام فالIPSec يحمي من معظم الهجمات عن طريق استخدامه ميكانيكية التشفير المعقدة ، حيث يوفر التشفير الحماية للبيانات والمعلومات أيا كانت أثناء انتقالها على الوسط (أيا كان) عن طريق عمليتي التشفير Encryption والهاش Hashing .

طريقة التشفير المستخدمة في الـIPSec :

عباره عن دمج لعدة Algorithms ومفاتيح حيث:

- Algorithm : عباره عن العملية الحسابية التي تمر فيها البيانات لكي تشفر
- Key : وهو عباره عن رقم(كود) سري يتم من خلاله قراءه أو تعديل أو حذف أو التحكم في البيانات المشفرة بشرط مطابقته للزوج الثاني الذي قام بعملية التشفير.

يطرأ سؤال على ذهن الجميع ، كيف يمكننا أن نستخدم ونستغل الIPSec ؟

الجـواب :يستخدم الIPSec عن طريق ما يعرف بالسياسات IPSec Policies والتي تطبق في الشبكة ، حيث أن كل مجموعة من القواعد التي تريد تطبيقها تشكل لنا سياسه، والIPSec يستخدم هذه النظرية ، الأمر الذي يجب الانتباه له هو اننا لا نستطيع عمل اكثر من سياسة لكل جهاز كمبيوتر ، لذلك يجب عليك تجميع كل القواعد والامور التي ترغب في تطبيقها في سياسه واحده تطبق على مستوى الاجهزه لا على مستوى الافراد .

قبل القيام بوضع القواعد وتطبيق السياسه ، يجب علينا مراعاة مايلي:

نوع الحركة Traffic Type :

حيث انك تقوم باستخدام الفلاتر لتحديد نوعية الحركة التي تريد أن تطبق عليها هذه القواعد ، فمثلا تستطيع ان تطبق فلتر يعمل على مراقبة بروتوكول HTTP و FTP فقط دون الباقي.

ماذا سيفعل الIPSec بعد التحقق من نوع الحركة Traffic :

بعد ذلك يجب أن نحدد للـــIPSec ماذا سيفعل بعد تطابق الترافيك مع الفلتر ، وهو ما يسمى Filter Action والذي تستخدمه لتخبر السياسة Policy ماذا ستفعل اذا تم مطابقة الترافيك حسب الفلتر، فمثلا يمكنك أن تجعل الIPSec يقوم بمنع الحركه على منفذ بروتوكول FTP ، وايضا تجعله يعمل على تشفير الحركه على منفذ بروتوكول HTTP . وأيضا تستطيع من خلال Filter Action



بتحديد أي أنظمة التشفير والهاش التي تريد أن تستخدمها Encryption and Hashing Algorithms في الشبكة السلكية.

- طريقة التحقق من الموثوقيه Authentication Method :

حيث يستخدم الIPSec ثلاث طرق للتحقق من الموثوقيه وهم :

- بروتوكول الكيربرس Kerberos Protocol
- الشهادات الإلكترونية Digital Certificates
- مشاركة مفتاح معين Preshared key

- استخدام احدى نظامي الIPSec وهما Tunnel or Transport mode (سبق تفصيلهما)
- نوع الاتصال أو الشبكة السلكية التي سيتم تطبيق السياسة عليها:

What connection type the rule applies to:

حيث ان السياسه يمكن ان تحدد الIPSec في نطاق الشبكة المحلية السلكية LAN ، أو أن يعمل على أساس الوصول من بعدRemote access أو ما يعرف بWAN ، أو الاثنين معا.

أما بالنسبة لطبقة النقل ، اذا كانت الشبكة محميه بواسطة جدار ناري Firewall فيجب عليك عمل الاتي:

فتح منفذ UDP 500

السماح بالProtocol Identifier (ID) number 51 for AH , number 50 for ESP

(مع الملاحظه ان رقم البروتوكول ID يختلف عن رقم المنفذ).

الـIntrusion Detection Systems: IDS :-

تقنية الIDS هي تقنية تساعد على تمييز الهجمات على الشبكات وهي تقنية مشابهة لأسلوب الكشف عن الفيروسات أو جرس الإنذار ضد اللصوص . والهدف منها إخبار مدير الشبكة بوجود دخيل محتمل suspected intrusion أو حدوث هجوم attack occurring .

أنواع الIDS:-

- ❖ Host_based : وهي تراقب الأنشطه على جهاز مضيف معين computer host أو أداة مثل الrouters لذا فأن عيبها هو أن الهجمات على أجهزة أخرى لن تستطيع رؤيتها.
- ❖ Network_based: وهي تراقب الحركة داخل الشبكة traffic بأسلوب مشابه لل packet sniffer حيث يمكنها تمييز الهجمات على إتصالات مشوشة أو غير شرعية ولكن ليس عبر الswitched network connections فتصميم الswitch قد يمنع من رؤية الهجمات على أنظمة متصلة عبر منفذ آخر.
- ❖ packet sniffer: هي برمجيات تستخدم في مراقبة وتحليل البيانات في شبكة محلية أو موسعة ويمكن إستخدامها للحصول على كلمات مرور ،محتويات بريد إلكتروني ،وتستخدم في الIDS لتحليل البيانات.

طرق كشف المتطفلين:

- Statistical : يستخدم النظام الإحصائي لدراسة الحركة على الشبكة ،وحدة المعالجة المركزية ،وتحميل الذاكرة memory loading لتحديد ما إذا كانت هناك هجمات تحدث، وهي معرضه لأن تعطي إنذارات كاذبة لكن ميزتها أنها تستطيع إكتشاف الهجمات الجديدة التي قد تمر دون ملاحظه في الطريقة الثانية.
- Signature: وتعتمد هذه الطريقة على قاعدة لتقنيات الهجمات حيث يبحث الIDSعن السلوك الذي يشير إلى نوع معين من السلوك المعرف لكن عيبه أنه لا يستطيع إكتشاف الهجمات غير المدرجه في قواعد البيانات.
- Neural: وتسمى neural based learning network والهدف منها إنشاء نظام تعليمي ليصبح هجين بين الطريقتين السابقتين.
- من أفضل التقنيات المستخدمه في الIDS هي عمل serverأو subnet كهدف مغري للهجوم والهدف منه أن يكون فخ فالهجمات على الفخ decoy target توفر إنذار مبكر للموظفين الملائمين ، الفخ يمكن أن يكون عالي التفاعل في بيئة مقلدة أو منخفض التفاعل مع مضيف ساكن .

طرق عمل الفخاخ :-

- جرة العسل honey pot: هي سيرفر لجذب إهتمام المهاجمين ، وهذا السيرفر ليس ذا قيمة في مجال العمل عدا أنه ينذر المنظمة بوقوع هجوم مستقبلاً.
- شبكة العسل honey net : وهي شبكة فرعية لجذب الإهتمام sacrificial subnet بها عدد قليل من الماكينات تم تصميمها لجذب إهتمام المهاجمين ، وأي مرور من شبكة العسل يعتبر مريب لأنه ليس هنالك أي نشاط إنتاجي حقيقي يحدث على هذه الشبكة والغرض من هذا التصميم هو أن يمنح رجال الأمن فرصة للحصول على إنذار مبكر بأن هنالك هجوم محتمل ضد بيئة الإنتاج الحقيقي.

حماية المكونات المادية :

فلترة الـMAC Address

الـــMAC Address او ال Media Access Control Address هو العنوان الفيزيائي لكروت الشبكة. كل كرت شبكة في العالم يحمل رقم يميزه عن غيره، تقوم الشركات المنتجة بوضع أرقام خاصة على أساس نظام الست عشري لتميز كروت الشبكة عن بعضها و من المفترض إن لا تكون هذه الأرقام مكررة أبداً. بطبيعة الحال نقطة الاتصال تعتبر من الطبقة الثانية في الOSI Model أو ال Open System Interconnect يعني في طبقة الـــــData Link كالمبدلات فان تعاملها يكون مع الMAC Address وليس مع الIP Address. و هنا يستطيع المسؤول عن الشبكة السلكية أن يحدد الأجهزة التي يسمح لها باستخدام نقطة الاتصال الخاصة به.

كما نعرف فان كل جهاز حتى يتصل بالشبكة يجب أن يحتوي على كرت شبكة السلكية-غالبا ما تكون موجودة في الجهاز من قبل الشركة المصنعة ، و كل كرت شبكة سلكية تملك رقم خاص مميز وهو الMAC Address و من المفترض أن المسؤول عن الشبكة السلكية يعي و يعلم عدد الأجهزة الموجودة لديه أو لدى شركته و التي يريدها أن تستخدم شبكته السلكية. و يحدد الأجهزة بواسطة إضافة أرقام الMAC الخاصة بهذه الأجهزة في قائمة الأجهزة المسموح لها باستخدام الشبكة

أو استخدام نقط الاتصال و لا يسمح بغير هذه الأجهزة مهما كانت باستخدام نقاط الاتصال الخاصة بشبكته.

طرق تأمين الكابلات :

لتأمين الكابلات من الموجات الكهرومغناطيسية أو من موجات الضجيج أو من تسلل بعض المتطفلين نقوم بعمل الحمايات اللازمة للكابل حسب نوعه :

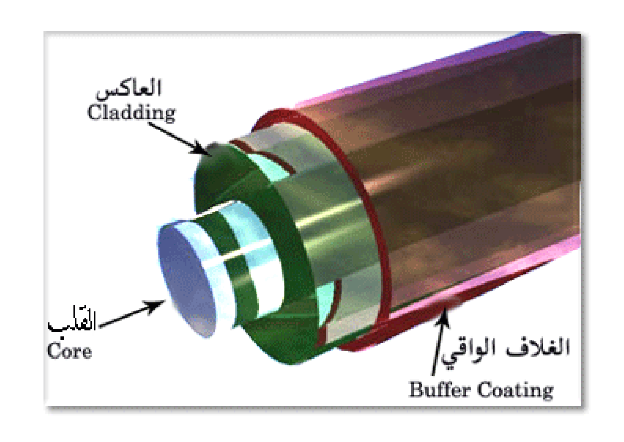
حماية الكابلات الضوئية Fiber Optic Cables :

١- كابلات الألياف الضوئية :

الألياف الضوئية هي:

عبارة عن أسلاك من الزجاج النقي وهي رقيقة – بمثل رقة شعر الإنسان – تحمل المعلومات الرقمية عبر مسافات طويلة. تركيب الألياف الضوئية

يتضمن تصنيع الألياف ثلاث عمليات رئيسية، هي:



١. تصنيع مادة الألياف.

٢. سحب الألياف ولفها على بكر خاص.

٣. قياس الخواص، الضوئية والآلية، للألياف وتحديدها.



١. إجراء تصنيع مادة الألياف

هناك وسائل عديدة لعملية التصنيع، تهدف جميعها إلى صهر مادة الزجاج، وتنقيتها من الشوائب، وجعلها سائلة. وتختلف هذه الوسائل بعضها عن بعض، في التكنولوجيات المستخدمة في عملية الصهر والتنقية، وفي الأغراض التي تُعَدّ لها.

٢. سحب الألياف

يلي سحب الألياف عملية تصنيع مادتها. ويجري السحب، والزجاج سائل ساخن؛ إذ تُلَفّ الألياف على بكر خاص، يدور بسرعة محسوبة، تعتمد على قطر الألياف المطلوب.

٣. قياس خواص الألياف وتحديدها

يُعْمَدَ إليه لتحديد الآتي:

- أ .القدرة الضوئية للألياف: وهي معدل مرور طاقه الضوء على نقطة معينة، في وقت محدد.
- ب .الاضمحلال: لتحديد مقدار الإشارة الضوئية، التي تفقد في الألياف.
- ج .عرض النطاق (B.W) ومعدل البيانات: ويعبران، أساساً، عن معكوس تشتت النبضة في الألياف.
- د .الفتحة الرقمية: (NA) وتحدد قدرة الألياف على التقاط الضوء الساقط على مدى كبير من الزوايا وتجميعه.
- هـــ .التشتت بأنواعه.
- و. طول الموجة النهائي:(Cut Off W. L) وعنده تبدأ الألياف في تداول النشاط الموجي الثاني (Second Mode) ، أي أنه يوضح حدود العمل الموجي للألياف.

٤.توصيل الألياف وتجميعها

الهدف منهما الوصول إلى نظام ألياف ضوئية متكامل. ويشمل ذلك الآتي:

أ. توصيل ألياف بألياف أخرى.

ب. توصيل المصدر الضوئي بالألياف.

ج. توصيل نهاية الألياف بالكواشف.

مكونات أنظمة الألياف الضوئية

١. كبل الألياف

بعد تصنيع الألياف وسحبها على البكر، فإنها تحتاج إلى طبقات حماية إضافية، حتى يمكن تداولها بسلام؛ ولذلك، تُجْعَل في كبيل. وعدد الألياف في الكبيل، يختلف باختلاف استخدام الكبل؛ فقد تكون شعيرة ليفية واحدة، أو عدة آلاف من الألياف.

وكبول الألياف الضوئية، تشابه الكبول المعدنية التقليدية؛ إلا أنها لا تحتاج إلى عزل كهربائي بين الألياف والكبول؛ إذ إن تلك الألياف غير موصلة، كهربائياً.

وكذلك، هي أصغر حجماً من الكبول المعدنية، ذات السعة نفسها من قنوات الاتصال؛ نظراً إلى قدرتها الفائقة على حمل العديد من القنوات، مجتمعة.

ويمكن تلخيص أسباب تصنيع الألياف في صورة كُبُل، في الآتي:

أ. لسهولة الاستخدام؛ إذ إن:

(١) صغر حجم الألياف، يجعلها صعبة التداول.

(٢) الألياف شفافة، يصعب رؤيتها على معظم الأسطح.

ب. الحماية، ضد الآتي:

(١) الإجهاد، على طول الألياف.

(٢) أي احتمالات للسحق، بالأقدام أو المركبات أو ضغط المياه، وخلافه.

(٣) تآكل الألياف وتعريتها.

خواص الألياف البصرية Properties of Optcal Fibers

٣-١ فتحة النفوذ التعددية Numerical Apertur

يتطلب اقتران الضوء في اللب البصري وقوع شعاع ضمن زاوية معينة تدعى زاوية القبول ويعبر عن قدرة تجميع الضوء يجيب Sine زاوية القبول والذي يطلق علية فتحة النفوذ العددية .

حيث أن no تمثل معامل انكسار الوسط الفاصل بين منبع الضوء والليف وn1 معامل انكسار اللب و n2 معامل انكسار الكساء . تحدد فتحة النفوذ العددية مقدار القدرة المقترنة بالليف .

٣-٢ التوهين Attenuation

يعتبر التوهين أحد العناصر الأساسية في تقويم أنظمة الاتصالات حيث تتعرض الموجات الحاملة للوهن عند انتشارها في قناة الاتصال نتيجة عوامل عديدة كالامتصاص Absorption والتناثر Scattering ويجب استخدام قنوات اتصال بأقل توهين ممكن حتى تنتشر الموجات الحاملة الأطول مسافة ممكنة . وفي قنوات الاتصال المصنعة من الألياف البصرية ، يلعب التوهين دوراً أساسياً في اختيار الليف ، وفقد الضوء في الليف البصري يعتمد الى حد كبير على الطول الموجي للضوء المستخدم حيث يقل عند بعض الأطوال الموجية ويزيد عند اطوال الموجية ويزيد عند اطوال موجية أخرى ، حيث أن امتصاص جزيئات (OH) للضوء يزداد عند بعض الأطوال الموجية ويقل عند أطوال موجية أخرى ، حيث أن امتصاص جزيئات (OH) للضوء يزداد مثلا عند طول موجي قدرة

١٣٩٠ نانومتر وتقاس قيمة التوهين لليف البصري بوحدة الديسيبل لتعبر عن النسبة بين الطاقة الضوئية المستقبلة والطاقة الضوئية المرسلة في الليف .

٣-٣ التشتيت Dispersion

التشتيت هو انبساط أو اتساع النبضة عند مرورها في قناة الاتصال وفي نظم الألياف البصرية ينقسم التشتيت الى نوعين وهما التشتيت النمطي Intermodal dispersionوالذي يتم نتيجة سلوك الاشارات المرسلة مساوات مختلفة عند انتشارها داخل الليف مما يؤدي الى عدم وصولها في وقت واحد . أما النوع الأخر فهو التشتيت الباطني وينقسم هذا التشتيت الى نوعين :

(أ) تشتيت المادة material dispersion

(ب) تشتيت الدليل الموجي waveguide dispersion

يحصل هذا النوع من التشتيتفي جميع أنواع الألياف البصرية وينتج من عرض خط المنبع البصري حيث أن المنابع البصرية لا تبث الضوء بطول موجي واحد بل بحزمة من الأطوال الموجية وحيث أن معامل انكسار الزجاج المستخدم في الألياف يتغير مع الطول الموجي فإن ذلك سيؤدي الى اختلاف في سرعة الاشارات أو النبضات مما يؤدي الى انبساطها ويؤثر ذلك على كمية المعلومات المراد نقلها .

✧ بعض أنواع الكابلات الضوئية المحمية:

أ. كبل داخلي، في معدة أو جهاز: ويكون صغير الحجم، بسيط التركيب، ورخيص الثمن.

ب. كبل بين المكاتب: للاستخدام داخل المبنى الواحد. ويحتوي، عادة، على شعيرة واحدة أو اثنتين من الألياف.

ج. كبل بين المباني: يمر على الجدران. ويحتوى على عدة ألياف.

هـــ. كبل خاص بين المباني، بمواصفات ضد الحريق والدخان.

و. كبل هوائي خارجي، بين أعمدة أو في أنفاق أرضية.

ز. كبل أنفاق مدرع.

ح. كبل الدفن المباشر، ذو طبقة خارجية مدرعة.

ط. كبل غواصات مائي: للاستخدام في المياه، العذبة أو المالحة.

عند عملية تصنيع الالياف الضوئية فان كلا الطبقتين تُصنعان معا ، وبعد ذلك تأتي منطقة الغلاف (Coating) وتتميز هذه الطبقة بانها طبقة خارجية تتم معالجتها بالاشعة فوق البنفسجية (UV) خلال عملية التصنيع ويتم تلوينها للتمييز بين الشعرات في نفس المجموعة وتكمن اهميتها بتأمين الحماية للشعرة نفسها ، يختلف سمك هذه الطبقة الا ان المتعارف عليه عالميا هو اما ٢٥٠ او ٩٠٠ ميكروميتر يستعمل السمك الاول غالبا من اجل الكوابل التي تستعمل خارج المباني في حين يستعمل السمك الثاني في الكوابل التي تستعمل داخل المباني .بعد ذلك يتم تصنيع ما يسمى ب (Buffer) وهي طبقة بلاستيكية تعمل كغلاف لمجموعة من الشعرات التي غالبا ما تصنع من مادة البلاستيك المعروف ب (PVC).

فيتم حمايتها من العوامل الطبيعية الخارجية و إلا فإنها أمنة من التدخلات الكهرومغناطيسية بسبب استخدامها للضوء في نقل البيانات.

حماية الكابلات المجدولة Twisted pair Cables :

هناك نوعين من الأسلاك المجدولة:

– المكشوفة

– و المحمية.

الأسلاك المجدولة المكشوفة

UTPهي الأكثر شيوعا وعادة أفضل اختيار لشبكات المكتبات الصغيرة.

تتراوح جودة الUTP من جودة سلك التليفون إلى جودة كابل فائق السرعة. يحتوي الكابل على أربعة أزواج من الأسلاك داخل الجاكت. كل زوج ملفوف بعدد مختلف من اللفات في البوصة الواحدة عن أي زوج آخر للتقليل من التشويش الذي قد يحدث نتيجة التقارب بين الأسلاك أو أجهزة كهربية أخرى interference. كلما كان اللف غير سميك ، كلما ازداد معدل نقل البيانات وكذلك ارتفاع تكلفة السلك.

بعض إرشادات الحماية للكابلات المجدولة Installation Guidelines :

- ✓ دائما استخدم كابل أطول مما تحتاج. أترك مساحة للمرونة.slack
- ✓ اختبر كل جزء من الشبكة بعد تحميله. حتى إن كان هذا الجزء جديد جدا ، فمن الممكن أن يكون به مشكلات يصعب عزلها لاحقا .
- ✓ ابعد على الأقل ثلاثة أقدام (حوالي متر) من صناديق ضوء الفلورسنت
- ✓ وأية مصادر أخرى للتشويش الكهربائي.



- ✓ إذا كان ضروريا مد الكابل عبر أرضية الغرفة ، غطي الكابل بحاميات
- ✓ الكابلات.
- ✓ عند بداية ونهاية كل كابل. ضع علامة label
- ✓ استخدم روابط الكابلاتللحفاظ على الكابلات معا في ذات المكان. cable tie (tape وليس شريط لاصق)

. حماية الكابلات المحورية Coaxial Cables :

تتكون الأسلاك المحورية في أبسط

صورها من التالي:

Coaxial Cable

Outer Jacket

Braided Copper Shielding

Copper Conductor

Plastic Insulation

BNC Connector

١. محور من النحاس الصلب محاط

٢. بمادة عازلة .

٣. ضفائر معدنية للحماية .

٤. غطاء خارجي مصنوع من

٥. المطاط أو البلاستيك أو التفلون

انظر الشكل جانبًا : .

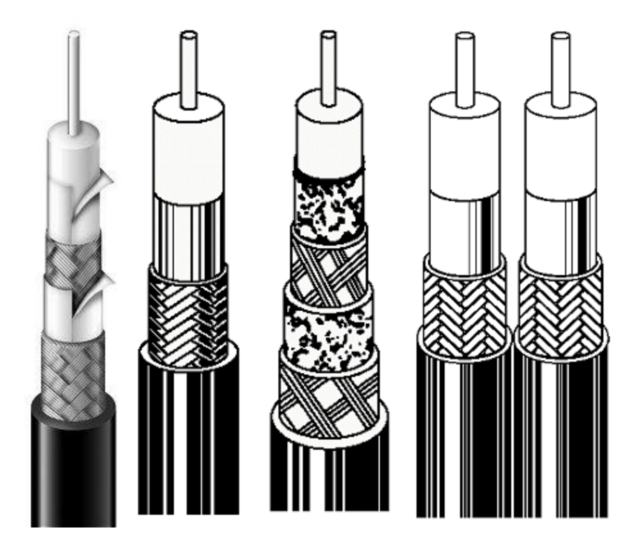
Teflon تقوم الضفائر (الشبكة) المعدنية بحماية

المحور من تأثير التداخل الكهرومغناطيسي Crosstalk و الإشارات التي تتسرب من الأسلاك

المجاورة أو ما يسمى EMI

إضافة لذلك تستخدم بعض الأسلاك المحورية طبقة أو طبقتين من القصدير كحماية إضافية .

و لابد من الأخذ في عين الاعتبار حماية الكابلات من دوائر القصر و إدراج حماية التحقق من المستقبل لحماية البيانات أثناء مرورها في الكابلات كما مر بنا في أمن طبقة الشبكة.





المراجع :

- http://www.arab-eng.org/vb/54745-post1.html#ixzz1gLcthn8U ملتقى المهندسين العرب
- مركز التميز لأمن المعلومات –جامعة الملك سعود– http://www.coeia.edu.sa
- موقع كتب http://www.kutub.info
- منتديات نظم القوى الكهربائية و شبكات النقل
- موقع تقريب علوم الشبكات للناطقين بلغة الضاد
- M. Ciampa, "Security+ Guide to Network Security Fundamentals",
- http://www.myegyptsun.com
- Security Measures in Wired and Wireless Networks
- Wired Network Security: Hospital Best Practices
  Jody Barnes - East Carolina University